Improved Power Decoding of One-Point Hermitian Codes

Puchinger, Sven ; Bouw, Irene; Rosenkilde, Johan Sebastian Heesemann

Published in:
Proceedings of International Workshop on Coding and Cryptography 2017

Publication date:
2017

Document Version
Peer reviewed version

Improved Power Decoding of One-Point Hermitian Codes

Sven Puchinger[1], Irene Bouw[2], and Johan Rosenkilde né Nielsen[3]

[1] Institute of Communications Engineering, Ulm University, Ulm, Germany
sven.puchinger@uni-ulm.de
[2] Institute of Pure Mathematics, Ulm University, Ulm, Germany
irene.bouw@uni-ulm.de
[3] Department of Applied Mathematics & Computer Science, Technical University of Denmark, Lyngby, Denmark
jsrn@jsrn.dk

Abstract. We propose a new partial decoding algorithm for one-point Hermitian codes that can decode up to the same number of errors as the Guruswami–Sudan decoder. Simulations suggest that it has a similar failure probability as the latter one. The algorithm is based on a recent generalization of the power decoding algorithm for Reed–Solomon codes and does not require an expensive root-finding step. In addition, it promises improvements for decoding interleaved Hermitian codes.

1 Introduction

One-point Hermitian (1-H) codes are algebraic geometry codes that can be decoded beyond half the minimum distance. Most of their decoders are conceptually similar to their Reed–Solomon (RS) code analogs, such as the *Guruswami–Sudan* (GS) algorithm [1] and *power decoding* (PD) [2–4]. For both RS and 1-H codes, PD is only able to correct as many errors as the Sudan algorithm, which is a special case of the GS algorithm. Recently [5], PD for RS codes was improved to correct as many errors as the GS algorithm.

In this paper, we combine the idea of improved power decoding (IPD) for RS codes from [5] with the description of PD for 1-H codes from [4] in order to obtain an IPD algorithm for 1-H codes. Similar to the RS case, we derive a larger system of non-linear key equations (cf. Section 3) than in classical PD and reduce the decoding problem to a linear Padé approximation problem whose solution is likely to agree with the solution of the system of key equations (cf. Section 4). Using a linear-algebraic argument, we derive an upper bound on the maximum number of errors which can possibly be corrected by the decoder (cf. Section 5). In Section 6, we show that the algorithm can be implemented with sub-quadratic complexity in the code length n. Finally, we present simulation results for various code and decoder parameters which indicate that the new IPD algorithm has a similar failure probability as the GS algorithm for the same parameters and decoding radius (cf. Section 7).

Besides the theoretical interest in having different decoding paradigms, we see two advantages of the new decoder: Firstly, the algorithm does not require a root-finding step, which is often considered to be computationally heavy, especially in practical implementations, see e.g. [6]. Secondly, the IPD algorithm for RS codes [5] was recently generalized to interleaved RS codes [7], where it improves upon existing decoding algorithms at all rates, including those methods which are based on the GS decoder. It is reasonable to assume that a similar generalization is also possible for 1-H codes.

2 Preliminaries

Let q be a prime power. We follow the notation of [4]. The *Hermitian curve* $\mathcal{H}/\mathbb{F}_{q^2}$ is the smooth projective plane curve defined by the affine equation $Y^q + Y = X^{q+1}$. The curve $\mathcal{H}(\mathbb{F}_{q^2})$ has genus $g = \frac{1}{2}q(q-1)$ and q^3+1 many $\mathbb{F}_{q^2}$-rational points $\mathcal{P} = \{P_1, \ldots, P_{q^3}, P_\infty\}$, where P_∞ denotes the point at infinity. We define $\mathcal{R} := \cup_{m\geq 0}\mathcal{L}(mP_\infty) = \mathbb{F}_{q^2}[X,Y]/(Y^q + Y - X^{q+1})$, which has an $\mathbb{F}_{q^2}$-basis of the form $\{X^iY^j : 0 \leq i, 0 \leq j < q\}$. The order function $\deg_{\mathcal{H}} : \mathcal{R} \to \mathbb{N}_0 \cup \{-\infty\}, f \mapsto -v_{P_\infty}(f)$ is defined by the valuation v_{P_∞} at P_∞. As a result, we have $\deg_{\mathcal{H}}(X^iY^j) = iq + j(q+1)$.

Let $n = q^3$ and $m \in \mathbb{N}$ with $2(g-1) < m < n$. The *one-point Hermitian code* of length n and parameter m over $\mathbb{F}_{q^2}$ is defined by

$$\mathcal{C}_{\mathcal{H}} = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(mP_\infty)\}\,.$$

The dimension of $\mathcal{C}_{\mathcal{H}}$ is given by $k = m - g + 1$ and the minimum distance d is lower-bounded by the *designed minimum distance* $d^* := n - m$.

3 System of Key Equations

In this section, we derive the system of key equations that we need for decoding, using the same trick as [5] for Reed–Solomon codes. We use the description of power decoding for one-point Hermitian codes as in [4]. Suppose that the received word is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_{q^2}^n$, consisting of an error $\boldsymbol{e} = (e_1, \ldots, e_n)$ and a codeword $\boldsymbol{c} \in \mathcal{C}_{\mathcal{H}}$, which is obtained from the *message polynomial* $f \in \mathcal{L}(mP_\infty)$. We denote the set of *error positions* by $\mathcal{E} = \{i : e_i \neq 0\}$.

In the following sections we show how to retrieve the message polynomial f from the received word $\boldsymbol{r}$ if the *number of errors*, the Hamming weight $\mathrm{wt_H}(\boldsymbol{e}) = |\mathcal{E}|$ of the error, does not exceed a certain decoding radius τ, which depends on the parameters of the decoding algorithm.

A non-zero polynomial $\Lambda \in \mathcal{L}\left(-\sum_{i\in\mathcal{E}} P_i + \infty P_\infty\right)$ is called *error locator*. It is well-known that there is an error locator of degree $|\mathcal{E}| \leq \deg_{\mathcal{H}} \Lambda \leq |\mathcal{E}| + g$, cf. [4]. and that any error locator fulfills $\deg_{\mathcal{H}}(\Lambda) \geq |\mathcal{E}|$ (cf. [4]). In this section, let Λ be some error locator.

Lemma 1 ([4, Lemma 6]). *There is a polynomial $R \in \mathcal{R}$ with $\deg_{\mathcal{H}}(R) < n + 2g$ that satisfies $R(P_i) = r_i$ for all $P_i \in \mathcal{P}^*$.*

In the following, let $R \in \mathcal{R}$ be as in Lemma 1 and $G \in \mathcal{R}$ be defined as

$$G = \prod_{\alpha \in \mathbb{F}_{q^2}} (X - \alpha) = X^{q^2} - X.$$

By [4, Theorem 24], we know that there is a unique *error evaluator polynomial* $\Omega \in \mathcal{R}$ that fulfills $\Lambda(R - f) = \Omega G$.

The following theorem states the system of key equations that we will use for decoding in the next sections. Note that the formulation is similar to its Reed–Solomon analog [5, Theorem 3.1], with the difference that all involved polynomials are elements of the ring $\mathcal{R}$.

Theorem 1 (System of Key Equations). *Let f, Λ, G, R, and Ω be as above, and $\ell, s \in \mathbb{N}$ such that $s \leq \ell$. Then, as a congruence over $\mathcal{R}$,*

$$\Lambda^s f^t = \sum_{i=0}^{t} \Lambda^{s-i} \Omega^i \tbinom{t}{i} R^{t-i} G^i \qquad \forall t = 1, \ldots, s-1, \tag{1}$$

$$\Lambda^s f^t \equiv \sum_{i=0}^{s-1} \Lambda^{s-i} \Omega^i \tbinom{t}{i} R^{t-i} G^i \mod G^s \qquad \forall t = s, \ldots, \ell. \tag{2}$$

Proof. We know that $\Omega G = \Lambda (f - R)$. Thus, for $s, t \in \mathbb{N}$, we have

$$\Lambda^s f^t = \Lambda^s \left(R + (f - R)\right)^t = \sum_{i=0}^{t} \tbinom{t}{i} \Lambda^s \left(f - R\right)^i R^{t-i}.$$

In all summands with $i < s$, we can rewrite $\Lambda^s (f - R)^i = \Lambda^{s-i} (\Lambda (f - R))^i = \Lambda^{s-i} (\Omega G)^i$. If $i \geq s$, $\Lambda^s (f - R)^i = (\Lambda (f - R))^s (f - R)^i = (\Omega G)^s (f - R)^{s-i}$, so all those summands are divisible by G^s, resulting in

$$\Lambda^s f^t = \sum_{i=0}^{\min\{t, s-1\}} \Lambda^{s-i} \Omega^i \binom{t}{i} R^{t-i} G^i + G^s \left(\sum_{i=\min\{t+1, s\}}^{t} \binom{t}{i} \Omega^s (f - R)^{s-i} R^{t-i} \right).$$

For $t < s$, we obtain (1) since the second part of the sum vanishes and for $t \geq s$, (2) holds because the latter sum is divisible by G^s. □

4 Solving the System of Key Equations

The idea of decoding is to find the message polynomial f from the known polynomials R and G. Since the system of key equations is non-linear in the unknown polynomials Λ, Ω, and f, we cannot solve it directly. Instead, we consider the following linearized problem, a *Padé approximation* problem.

Problem 1. Let G and R be as in Section 3. Given $\tau \in \mathbb{N}$ and

$$a^{(t,i)} := \binom{t}{i} R^{t-i} G^i, \quad G_t := \begin{cases} x^{\lfloor \frac{t(n+2g-1)+\tau}{q} \rfloor + 1}, & \forall t = 1, \ldots, s-1, \\ G^s, & \forall t = s, \ldots, \ell, \end{cases}$$

for all $i = 0, \ldots, s-1$ and $t = 1, \ldots, \ell$, find a vector

$$(\lambda^{(0)}, \ldots, \lambda^{(s-1)}, \psi^{(1)}, \ldots, \psi^{(\ell)}) \in \mathcal{R}^{s+\ell} \setminus \{\mathbf{0}\},$$

with minimal $\deg_{\mathcal{H}}(\lambda^{(0)})$ which satisfies

$$\sum_{i=0}^{s-1} \lambda^{(i)} a^{(t,i)} \equiv \psi^{(t)} \mod G_t \qquad \forall t = 1, \ldots, \ell, \tag{3}$$

$$\deg_{\mathcal{H}}(\lambda^{(i)}) \leq s\tau + i(2g-1) \qquad \forall i = 0, \ldots, s-1, \tag{4}$$

$$\deg_{\mathcal{H}}(\psi^{(t)}) \leq s\tau + tm \qquad \forall t = 1, \ldots, \ell, \tag{5}$$

where the congruences are over $\mathcal{R}$.

The following theorem motivates the statement of Problem 1 by showing that the polynomials $\Lambda^{s-i}\Omega^i$ and $\Lambda^s f^t$ that occur in the key equation fulfill the congruences and degree constraints of the problem. The minimality condition ensures that if the problem solution corresponds to an error locator Λ of some error vector $\boldsymbol{e}$ (not necessarily the same $\boldsymbol{e}$ as in Section 3), i.e., $\lambda^{(0)} = \Lambda^s$, then it is the one of smallest degree, and thus hopefully the one corresponding to the $\boldsymbol{e}$ of smallest Hamming weight.

The theorem also implies a strategy to obtain f after having solved Problem 1: If the solution of Problem 1 results in $\lambda^{(0)} = \Lambda^s$ and $\psi^{(1)} = \Lambda^s f$ for some error locator Λ, we divide $\psi^{(1)}$ by $\lambda^{(0)}$. See [4] for how this division can be performed.

Theorem 2. *Let f, Λ, G, R, and Ω be as in Section 3, and $\ell, s \in \mathbb{N}$ such that $s \leq \ell$. For $t = 1, \ldots, \ell$ and $i = 0, \ldots, s-1$, we define the polynomials (all in $\mathcal{R}$)*

$$\Lambda^{(i)} := \Lambda^{s-i}\Omega^i, \quad \Psi^{(t)} := \Lambda^s f^t,$$

Then, $(\Lambda^{(0)}, \ldots, \Lambda^{(s-1)}, \Psi^{(1)}, \ldots, \Psi^{(\ell)})$ satisfies Conditions (3) - (5) *of Problem 1 for any $\tau \geq \deg_{\mathcal{H}}(\Lambda)$.*

Proof. Inequality (4) is fulfilled since

$$\deg_{\mathcal{H}}(\Omega) = \deg_{\mathcal{H}}(\Omega G) - n = \deg_{\mathcal{H}}(\Lambda(f - R)) - n \leq \tau + 2g - 1.$$

Also, Inequality (5) holds due to $\deg_{\mathcal{H}}(f) \leq m$ and

$$\deg_{\mathcal{H}}(\Psi^{(t)}) = \deg_{\mathcal{H}}(\Lambda^s) + \deg_{\mathcal{H}}(f^t) \leq s\tau + tm.$$

Condition (3) is satisfied by Theorem 1 (note that $a^{(t,i)} = 0$ for $i > t$ and that the congruence modulo $x^{\lfloor \frac{t(n+2g-1)+\tau}{q} \rfloor + 1}$ in (3) is the same as equality due to the degree restrictions). □

5 Decoding Radius and Failure Behavior

As any other power decoder, the new decoding algorithm is a partial decoding algorithm, which means that it might fail for certain error patterns. This failure behavior has many reasons that we would like to discuss in this section. We start by deriving a bound on the parameter τ of Problem 1 that ensures the problem to have a solution.

Theorem 3. *Problem 1 is guaranteed to have a solution if*

$$\tau \geq \tau_{\text{new}} := n\left[1 - \tfrac{s+1}{2(\ell+1)}\right] - \tfrac{\ell}{2s}m - \tfrac{\ell-s+1}{s(\ell+1)} + \tfrac{g-1}{\ell+1}.$$

Proof. Problem 1 is guaranteed to have a solution if there at least one vector

$$(\lambda^{(0)}, \ldots, \lambda^{(s-1)}, \psi^{(1)}, \ldots, \psi^{(\ell)}) \in \mathcal{R}^{s+\ell} \setminus \{\mathbf{0}\},$$

satisfying Conditions (3), (4), and (5). We can find such a solution by solving the following homogeneous linear system of equations in the coefficients of the $\lambda^{(i)}$, which we consider these coefficients as indeterminates. Since $\deg_{\mathcal{H}}(\psi^{(t)}) \leq s\tau + tm$ (cf. (5)), the coefficients of $\sum_{i=0}^{s-1} \lambda^{(i)} a^{(t,i)}$ in (3) of degree greater than $s\tau + tm$ and less than

$$T_t := \begin{cases} t(n+2g-1) + s\tau + 1, & t = 1, \ldots, s-1, \\ \deg_{\mathcal{H}}(G^s), & t = s, \ldots, \ell, \end{cases}$$

must be zero. Since we require $\deg_{\mathcal{H}} \lambda^{(i)} \leq s\tau + i(2g-1)$, see (4), there at at least $s\tau + i(2g-1) - g + 1$ indeterminates for $\lambda^{(i)}$. After obtaining non-zero polynomials $\lambda^{(i)}$, we can find $\psi^{(t)}$ by computing $\sum_{i=0}^{s-1} \lambda^{(i)} a^{(t,i)}$ modulo G_t.

It suffices to show that the described system has a non-zero solution for $\tau \geq \tau_{\text{new}}$. The system has at most

$$\begin{aligned} E &= \textstyle\sum_{t=1}^{\ell} [T_t - (s\tau + tm) - 1] \\ &\leq ns\left[\ell + 1 - \tfrac{s+1}{2}\right] - \tfrac{\ell(\ell+1)}{2}m + \tfrac{s(s-1)}{2}(2g-1) + \tau s(s-1-\ell) - (\ell - s + 1) \end{aligned}$$

equations and at least

$$V = \textstyle\sum_{i=0}^{s-1} [s\tau + i(2g-1) - g + 1] = s^2\tau + \tfrac{s(s-1)}{2}(2g-1) - sg + s$$

indeterminates. Thus, it has a non-zero solution if $V \geq 1 + E$, which can be re-written as $\tau \geq \tau_{\text{new}}$. □

Theorem 3 can be interpreted as follows. For some $\tau \in \mathbb{N}$, we denote by $\mathcal{V}_\tau$ the $\mathbb{F}_{q^2}$-vector space consisting of all vectors

$$(\lambda^{(0)}, \ldots, \lambda^{(s-1)}, \psi^{(1)}, \ldots, \psi^{(\ell)}) \in \mathcal{R}^{s+\ell}$$

that satisfy the congruences and degree constraints of Problem 1 with parameter τ. If we choose $\tau \geq \tau_{\text{new}}$, then $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_\tau) \geq 1$. In addition, if $\tau \geq \deg_{\mathcal{H}}(\Lambda)$, then

$$(\Lambda^s, \Lambda^{s-1}\Omega, \ldots, \Lambda\Omega^{s-1}, \Lambda^s f, \Lambda^s f^2, \ldots, \Lambda^s f^\ell) \in \mathcal{V}_\tau.$$

Hence, if there is a τ with $|\mathcal{E}| \leq \deg \Lambda \leq \tau \leq \tau_{\text{new}}$ and $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_\tau) = 1$, a non-trivial solution of Problem 1 must yield a solution $(\Lambda^s, \Lambda^s f)$ of the decoding problem. Thus, we could expect that at least in some cases, we can decode up to $|\mathcal{E}| \leq \tau_{\text{new}}$ errors. However, there are several problems that could prevent us from correcting τ_{new} many errors:

i) The minimal degree of an error locator is greater than $|\mathcal{E}|$. Recall that it is only guaranteed that there is an error locator of $\deg_{\mathcal{H}} \Lambda \leq |\mathcal{E}| + g$.

ii) We get $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_\tau) > 1$ already for some $\tau < \tau_{\text{new}}$. This can have two reasons:
   - The number of equations is smaller than E (as in the proof of Theorem 3), which can be the case if $\deg_{\mathcal{H}} R < n + 2g - 1$.
   - The equations are linearly dependent.

iii) There is no τ with $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_\tau) = 1$ (e.g., if there is a τ with $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_\tau) = 0$ and $\dim_{\mathbb{F}_{q^2}}(\mathcal{V}_{\tau+1}) > 1$) and there is a "smaller" solution (corresponding to another codeword or a generic one) in $\mathcal{V}_\tau$ than $(\Lambda^s, \ldots, \Lambda\Omega^{s-1}, \Lambda^s f, \ldots, \Lambda^s f^\ell)$.

We will see in the Section 7 that in our experiments, for all tested examples, we were able to correct up to $n[1 - \frac{s+1}{2(\ell+1)}] - \frac{\ell}{2s}m - \frac{\ell-s+1}{s(\ell+1)} = \tau_{\text{new}} - \frac{g-1}{\ell+1}$ many errors with high probability. This number of errors coincides with the classical power decoding radius for $s = 1$, cf. [4].

6 Complexity

In this section, we show that Problem 1 can be solved in sub-quadratic time in the code length n. We use the algorithm in [8], which computes, for given $S_{\boldsymbol{i},\boldsymbol{j}} \in \mathbb{F}_{q^2}$, $G_{\boldsymbol{j}} \in \mathbb{F}_{q^2}[X]$, $T_{\boldsymbol{i}} \in \mathbb{N}$, and $N_{\boldsymbol{i}} \in \mathbb{N}$, where $\boldsymbol{i} \in I$ and $\boldsymbol{j} \in J$ (index sets), a basis (the solution space is a vector space) of all solutions $\lambda_{\boldsymbol{i}}, \psi_{\boldsymbol{j}} \in \mathbb{F}_{q^2}[X]$, that fulfill

$$\begin{aligned} &\sum_{\boldsymbol{i} \in I} \lambda_{\boldsymbol{i}} \equiv \psi_{\boldsymbol{j}} \mod G_{\boldsymbol{j}} && \forall \boldsymbol{j} \in J, \\ &\deg \lambda_{\boldsymbol{i}} \leq N_{\boldsymbol{i}} && \forall \boldsymbol{i} \in I, \\ &\deg \psi_{\boldsymbol{i}} \leq T_{\boldsymbol{i}} && \forall \boldsymbol{j} \in J, \end{aligned}$$

in $O^{\sim}\left(|J|^{\omega-1} \cdot |I| \cdot \max_{\boldsymbol{j}}\{\deg G_{\boldsymbol{j}}\}\right)$ operations over $\mathbb{F}_{q^2}$, where ω is the matrix multiplication exponent.

We use the $\mathbb{F}_{q^2}[X]$-vector representation of an element of $\mathcal{R}$ (cf. [4]) to reformulate Problem 1 as a problem of the type above. Recall that for $a \in \mathcal{R}$, we

can write $a = \sum_{i=0}^{q-1} a_i Y^i \in \mathcal{R}$ with unique $a_i \in \mathbb{F}_{q^2}[X]$. Then, the *vector representation* [4] of a is defined by $\boldsymbol{\nu}(a) = (a_0, \ldots, a_{q-1}) \in \mathbb{F}_{q^2}[X]^q$. Note that $q \deg(a_i) + i(q+1) \leq \deg_{\mathcal{H}}(a)$. For $a, b \in \mathcal{R}$ it can be shown that

$$\boldsymbol{\nu}(a+b) = \boldsymbol{\nu}(a) + \boldsymbol{\nu}(b), \qquad \boldsymbol{\nu}(ab) = \boldsymbol{\nu}(a)\boldsymbol{\mu}(b)\boldsymbol{\Xi},$$

where $\boldsymbol{\mu}(b) \in \mathbb{F}_{q^2}[X]^{q \times (2q-1)}$ and $\boldsymbol{\Xi} \in \mathbb{F}_{q^2}[X]^{(2q-1)\times q}$ are defined by

$$\boldsymbol{\mu}(b) := \begin{bmatrix} b_0 & b_1 & b_2 & \ldots & b_{q-1} & & \\ & b_0 & b_1 & \ldots & b_{q-2} & b_{q-1} & \\ & & \ddots & \ddots & \ldots & \ddots & \ddots \\ & & & b_0 & b_1 & \ldots & b_{q-2} \; b_{q-1} \end{bmatrix}, \quad \boldsymbol{\Xi} := \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ X^{q+1} & -1 & & \\ & X^{q+1} & -1 & \\ & \ddots & \ddots & \\ & & X^{q+1} & -1 \end{bmatrix}.$$

Using this notation, we define $\boldsymbol{A}^{(t,i)} := \boldsymbol{\mu}(a^{(t,i)})\boldsymbol{\Xi} \in \mathbb{F}_{q^2}[X]^{q\times q}$. We are ready to state the final complexity result.

Theorem 4. *Problem 1 can be solved using the algorithm in [8] with*

$$I = \{(i,j) : i \in \{0,\ldots,s-1\},\, j \in \{0,\ldots,q-1\}\}, \qquad S_{(i,j),(t,r)} = A^{(t,i)}_{j,r},$$
$$J = \{(t,r) : t \in \{1,\ldots,\ell\},\, r \in \{0,\ldots,q-1\}\}, \qquad G_{(t,r)} = G_t,$$
$$N_{(i,j)} = \tfrac{s\tau + i(2g-1) - j(q+1)}{q}, \quad T_{(t,r)} = \tfrac{s\tau + tm - r(q+1)}{q}$$

in $O^{\sim}(\ell^{\omega-1} s^2 n^{\frac{\omega+2}{3}})$ operations over $\mathbb{F}_q$, where the $O^{\sim}$ hides $\log(ns\ell)$ factors.

Proof. Similar to [4], pre-computing the matrices $\boldsymbol{A}^{(t,i)}$ is negligible compared to solving the Padé approximation problem. By the properties of $\boldsymbol{\nu}(\cdot)$, it is clear that $\lambda^{(i)}, \psi^{(t)} \in \mathcal{R}$ solve Problem 1 if and only if $(\lambda_{(i,0)}, \ldots, \lambda_{(i,q-1)}) = \boldsymbol{\nu}(\lambda^{(i)})$ and $(\psi_{(t,0)}, \ldots, \psi_{(t,q-1)}) = \boldsymbol{\nu}(\psi^{(t)})$ correspond to a non-zero element in the output of the algorithm in [8] of minimal $\max_{j\in\{0,\ldots,q-1\}} \left\{ q \deg(\lambda_{(0,j)}) + (q+1)j \right\}$. Since $\deg G_t \leq \lfloor \frac{t(n+2g-1)+\tau}{q} \rfloor + 1 \in O(sn/q)$, a basis of the solution space is found in

$$O^{\sim}\left((\ell q)^{\omega-1}(sq)(sn)\right) = O^{\sim}\left(\ell^{\omega-1} s^2 q^{\omega-1} n\right) = O^{\sim}\left(\ell^{\omega-1} s^2 n^{\frac{\omega+2}{3}}\right).$$

The algorithm in [8] outputs a reduced basis, so a minimal element is guaranteed to be one of the basis elements. □

Note that for constant parameters ℓ, s, the complexity in Theorem 4 is subquadratic in the code length n. We achieve the same complexity[4] as the algorithms in [4].

[4] The exponent of ℓ in the complexity statements in [4] is ω. If we apply the algorithm from [8] to these methods, we will also get $\omega - 1$.

7 Numerical Results

In this section, we present simulation results. We have conducted Monte-Carlo simulations for estimating the failure probability of the new improved power ($\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$) and the Guruswami–Sudan ($\hat{\mathrm{P}}_{\mathrm{fail,GS}}$) decoder in a channel that randomly adds τ errors, using a sample size $N \in \{10^3, 10^4\}$. The decoder was implemented in SageMath v7.5 [9], based on the power decoder implementation of [4]. We used the Guruswami–Sudan decoder implementation from [4].

Table 1. Observed failure rate of the improved power ($\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$) and Guruswami–Sudan ($\hat{\mathrm{P}}_{\mathrm{fail,GS}}$) decoder. Code parameters q, m, n, k, d^*. Decoder parameters ℓ, s. Number of errors τ (*decoding radius as in (6)). Number of experiments N.

q	m	n	k	d^*	ℓ	s	τ	$\hat{\mathrm{P}}_{\mathrm{fail,IPD}}$	$\hat{\mathrm{P}}_{\mathrm{fail,GS}}$	N
4	15	64	10	49	4	2	28	0	0	10^4
							29^*	0	$3.30 \cdot 10^{-3}$	10^4
							30	$9.93 \cdot 10^{-1}$	$9.39 \cdot 10^{-1}$	10^4
5	55	125	46	70	3	2	34	0	0	10^4
							35	0	0	10^4
							36^*	0	$4.00 \cdot 10^{-4}$	10^4
5	20	125	11	105	5	2	67	0	0	10^3
							68^*	0	$7.00 \cdot 10^{-3}$	10^3
							69	$9.91 \cdot 10^{-1}$	$9.60 \cdot 10^{-1}$	10^3
7	70	343	50	273	3	2	160	0	0	10^3
							161^*	0	0	10^3
							162	$9.78 \cdot 10^{-1}$	$9.86 \cdot 10^{-1}$	10^3
7	70	343	50	273	4	2	168	0	0	10^3
							169^*	0	0	10^3
							170	$9.79 \cdot 10^{-1}$	$2.2 \cdot 10^{-2}$	10^3
							171	1	1	10^3
7	55	343	35	288	4	2	184^*	0	0	10^3
							185	$9.82 \cdot 10^{-1}$	$1.9 \cdot 10^{-2}$	10^3
							186	1	1	10^3

Table 1 presents the simulation results for various code (q, m, n, k, d^*), decoder (ℓ, s), and channel (τ) parameters. It can be observed that both algorithms can almost always correct

$$\tau = n\left[1 - \tfrac{s+1}{2(\ell+1)}\right] - \tfrac{\ell}{2s}m - \tfrac{\ell-s+1}{s(\ell+1)} \tag{6}$$

errors, improving upon classical power decoding. Also, none of the two algorithms is generally superior.

8 Conclusion

We have presented a new decoding algorithm for one-point Hermitian codes which is based on the improved power decoder for Reed–Solomon codes from [5]. Experimental results indicate that the new algorithm has a similar failure probability as the Guruswami–Sudan algorithm at the same decoding radius.

A generalization of the new algorithm to interleaved one-point Hermitian codes, similar to [7], promises improved decoding radii for interleaving degrees $m > 1$ compared to existing decoding algorithms, and is work in progress.

References

1. V. Guruswami and M. Sudan, "Improved Decoding of Reed–Solomon and Algebraic-Geometric Codes," in *Annual Symposium on Foundations of Computer Science*. IEEE, 1998, pp. 28–37.
2. G. Schmidt, V. R. Sidorenko, and M. Bossert, "Syndrome Decoding of Reed–Solomon Codes Beyond Half the Minimum Distance Based on Shift-Register Synthesis," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5245–5252, 2010.
3. S. Kampf, "Decoding Hermitian Codes - An Engineering Approach," Ph.D. dissertation, Universität Ulm, 2012.
4. J. S. R. Nielsen and P. Beelen, "Sub-Quadratic Decoding of One-Point Hermitian Codes," *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3225–3240, 2015.
5. J. S. R. Nielsen, "Power Decoding Reed–Solomon Codes up to the Johnson Radius," *Submitted to: Advances in Mathematics of Communications*, 2016, arXiv preprint arXiv:1505.02111.
6. A. Ahmed, R. Koetter, and N. R. Shanbhag, "VLSI Architectures for Soft-Decision Decoding of Reed–Solomon Codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 648–667, 2011.
7. S. Puchinger and J. Rosenkilde né Nielsen, "Decoding of Interleaved Reed-Solomon Codes Using Improved Power Decoding," *Submitted to ISIT 2017, arXiv preprint arXiv:1701.06555*, 2017.
8. J. Rosenkilde né Nielsen and A. Storjohann, "Algorithms for Simultaneous Hermite Padé Approximations," *In preparation. Extended version of [?].*
9. W. A. Stein *et al.*, "SageMath Software," http://www.sagemath.org.